

⑯ BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

⑯ Offenlegungsschrift
⑯ DE 195 08 722 A 1

⑯ Int. Cl. 6:
G 06 K 19/073

DE 195 08 722 A 1

⑯ Aktenzeichen: 195 08 722.4
⑯ Anmeldetag: 10. 3. 95
⑯ Offenlegungstag: 12. 9. 96

⑯ Anmelder:
Siemens AG, 80333 München, DE

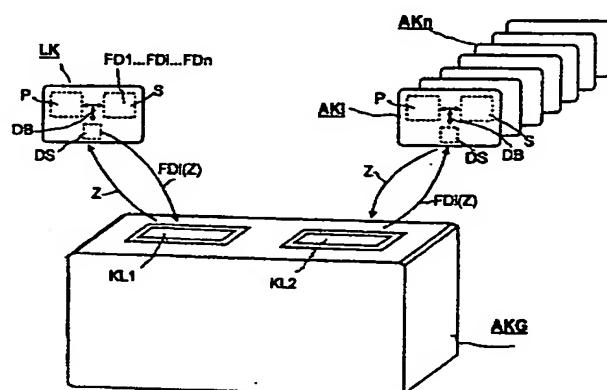
⑯ Erfinder:
Weinländer, Markus, 91230 Happurg, DE

⑯ Entgegenhaltungen:
DE 30 41 393 C2
DE 41 15 152 A1

Prüfungsantrag gem. § 44 PatG ist gestellt

⑯ Lizenzkartengesteuertes Chipkartensystem

⑯ Die Erfindung betrifft ein Chipkartensystem, dessen Chipkarten (AK, LK) jeweils mindestens einen internen Prozessor (P) und einen nichtflüchtigen Speicher (S) zumindest für ein Betriebssystem des Prozessors (P) aufweisen. Es sind eine Vielzahl von Anwenderchipkarten (AKn) vorhanden, deren Prozessoren (P) jeweils erst nach einer Freischaltung Anwenderbefehlsanweisungen ausführen können, und zumindest eine Lizenzchipkarte (LK), in deren nichtflüchtigen Speicher (S) eine begrenzbare Anzahl von freischaltbaren Anwenderchipkarten (AKn) verwaltbar ist. Mittels mindestens einer Schreib-Lesestation (AKG) für Chipkarten (LK) wird in einer Anwenderchipkarte (AKi) die Freischaltung des internen Prozessors (P) bewirkt, wenn im Speicher (S) der Lizenzchipkarte (LK) die Anzahl der freischaltbaren Anwenderchipkarten (AKn) noch nicht erschöpft ist. Anschließend erfolgt im Speicher (S) der Lizenzchipkarte (LK) eine Dekrementierung der Anzahl freischaltbarer Anwenderchipkarten (AKn).



DE 195 08 722 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 07. 98 602 037/508

8/24

Beschreibung

Chipkarten finden in stark steigendem Maße in unterschiedlichsten Bereichen des täglichen Lebens Anwendung. Dementsprechend sind sehr große Mengen derselben im Umlauf. Üblicherweise sind eine Vielzahl von Maßnahmen vorgesehen, um nach der Ausgabe der Chipkarte, d. h. während der normalen Benutzung, Vermögensschäden insbesondere für den jeweiligen Kartenbesitzer zu vermeiden. So muß z. B. nach einem Kartenverlust zumindest eine unbefugten Benutzung der Karte durch beliebige Dritte verhindert werden.

Aufgrund der steigenden mengenmäßigen Verbreitung müssen aber auch Maßnahmen vorgesehen werden, um einerseits insbesondere größere Kartenmengen bereits vor deren einzelner Ausgabe an die Endkunden zu schützen, und andererseits die Menge der legal an Endkunden ausgegebenen bzw. z. B. pro Zeitraum oder einem an einen Lizenzgeber bzw. Dienstleistungsbereitsteller aktuell entrichteten Vergütungsbetrag maximal ausgebbaften Karten zu überwachen bzw. zu begrenzen.

So werden Karten z. B. in u. U. sehr großen Mengen von einem Kartenhersteller an einen Verteiler von Karten, z. B. an ein Geldinstitut geschickt. Dieser Weg ist vergleichbar mit dem Transport von größeren Geldmengen zwischen Banken, und somit entsprechend gefährdet. Ferner ist es vielfach wünschenswert, auch auf Seiten des Verteilers von Karten, die Anzahl der z. B. pro Angestellten an Endkunden herausgebaren Karten genau zu überwachen, zu dokumentieren und zu begrenzen, um auch hierbei die Gefahr von Mißbrauch möglichst auszuschließen. Da in der Regel mit der Abgabe einer Karte an einen Endkunden die Inanspruchnahme von Leistungen durch diesen ermöglicht wird, können durch Chipkarten, welche unter Umständen in erhöhter Menge unzulässigerweise in den Umlauf gebracht worden sind, erhebliche Vermögensschäden entstehen.

Der Erfahrung liegt die Aufgabe zugrunde, ein Chipkartensystem anzugeben, bei dem einerseits die Anzahl der in den Umlauf bringbaren Chipkarten genau beeinflußt werden kann, und bei dem andererseits die normale, volle Funktionalität einer jeden Chipkarte erst durch zusätzliche, insbesondere im Moment von deren Ausgabe an einen Endbenutzer auszuführende Anpassungen, herstellbar ist.

Die Aufgabe wird gelöst mit dem im Anspruch 1 angegebenen Chipkartensystem. Vorteilhafte weitere Ausgestaltungen desselben sind in den Unteransprüchen enthalten.

Die Erfahrung und vorteilhafte weitere Ausgestaltungen desselben werden anhand der nachfolgend kurz angeführten Figuren näher erläutert. Dabei zeigt

Fig. 1 ein schematisches Strukturbild des erfundungsgemäßen Chipkartensystems, und

Fig. 2 eine bevorzugte Ausführungsform des Chipkartensystems, bei der zur Freischaltung einer Anwenderchipkarte ein von dessen Betriebssystem für die Ausführung von Anwenderbefehlsanweisungen benötigten Freigabedatensatzes in den nichtflüchtigen Speicher geladen wird.

Das erfundungsgemäße Chipkartensystem verfügt prinzipiell über zwei Typen von Chipkarten. Zum einen sind sogenannte Anwenderchipkarten AKn in der Regel in einer sehr großen Vielzahl vorhanden. Im Beispiel der Fig. 1 sind einige davon rechts oben aufgefächert dargestellt, wobei zur weiteren Erläuterung auf die im Vordergrund dargestellte Anwenderchipkarte AKi Bezug

genommen wird. Erfahrungswesentlich ist ein weiterer Chipkartentyp vorhanden, welcher die Funktion einer Freischaltkarte hat und im Folgenden als sogenannte Lizenzkarte bezeichnet werden soll. Von diesem Chip-

5 kartentyp sind naturgemäß nur sehr wenige im Besitz von ausgewählten, besonders legitimierten Personen. Möglicherweise ist sogar nur eine einzige derartige Karte im Umlauf. Im Beispiel der Fig. 1 ist eine derartige Lizenzchipkarte LK links oben dargestellt.

10 Vorteilhaft sind alle Karten des Chipkartensystems hardwaremäßig identisch, und unterscheiden sich in der Art des jeweils ausführbaren Anwenderprogrammes. Hierdurch wird die Herstellung der Chipkarten des Systems erheblich vereinfacht. Dementsprechend verfügen im Beispiel der Fig. 1 sowohl die Anwenderchipkarten AKi als auch die beispielhaft eine Lizenzchipkarte LK über die gleichen Hardwareelemente. Diese sind jeweils im wesentlichen ein interner Prozessor P, ein nichtflüchtiger Speicher S zumindest zur Aufnahme für 15 ein Betriebssystem des Prozessors P, eine Schnittstelle DS zum Datenaustausch mit einer Schreib-Lesestation AKG, welche z. B. in Form eines Kontaktfelds zum berührungsbehafteten Datenaustausch oder in Form einer Antenne zum berührungslosen Datenaustausch ausgeführt sein kann, und chipkarteninterner Datenbus DS.

20 Gemäß der Erfahrung sind die Anwenderchipkarten AKn so organisiert, daß deren Prozessor P jeweils erst nach einer Freischaltung Anwenderbefehlsanweisungen ausführen kann, während im nichtflüchtigen Speicher S 25 der zumindest einen Lizenzkarte LK eine begrenzbare Anzahl von freischaltbaren Anwenderchipkarten AKn verwaltbar ist. Schließlich verfügt das erfundungsgemäß 30 Chipkartensystem über mindestens eine Schreib-Lesestation AKG für Chipkarten LK bzw. AKn, worüber in einer Anwenderchipkarte AKi die Freischaltung des internen Prozessors P wirkt wird, wenn im Speicher S der Lizenzkarte LK die maximale Anzahl der freischaltbaren Anwenderchipkarten Akn noch nicht erschöpft ist. Nach einer erfolgreichen Freischaltung wird im 35 Speicher S der Lizenzchipkarte LK wiederum mit Hilfe der Schreib-Lesestation AKG eine Dekrementierung der Anzahl freischaltbarer Anwenderchipkarten Akn bewirkt.

Zum Datenaustausch zwischen einer Lizenzchipkarte 40 LK und einer aktuell zu bearbeitenden Anwenderchipkarte AK müssen beide Chipkarten z. B. bei einer berührungslosen Datenübertragung in den Sendebereich der Schreib-Lesestation AKG gebracht werden. Bei einem berührungsbehafteten Datenaustausch kann es 45 notwendig sein, die Chipkarten u. U. sukzessive mehrmals abwechselnd in die Schreib-Lesestation AKG einzuführen und wieder zu entnehmen. Bei der in Fig. 1 dargestellten Ausführung weist die Schreib-Lesestation AKG beispielsweise zwei Kartenleseeinheiten auf. Die 50 erste Kartenleseeinheit KL1 dient zur Aufnahme der Lizenzchipkarte LK, während die zweite Kartenleseeinheit KL2 zur Aufnahme einer Anwenderchipkarte AKi dient. In einem solchen Fall ist für eine Freischaltung einer Anwenderchipkarte vorteilhaft kein Wechsel von Chipkarten notwendig.

Bei einer bevorzugten Ausführungsform der Erfahrung wird vom Prozessor P einer Anwenderchipkarte AKi zur Auslösung einer Freischaltung zunächst eine Zufallszahl Z erzeugt und mittels der Schreib-Lesestation AKG an die Lizenzchipkarte LK übertragen. Ein 55 derartiger Fall ist im Beispiel der Fig. 1 mit Hilfe von gekrümmten Pfeilen dargestellt, welche die jeweilige Richtung des Datenüberganges zwischen der Daten-

BEST AVAILABLE COPY

schnittstelle DS der jeweiligen Chipkarte und der Schreib-Lesestation AKG anzeigen. So wird eine Zufallszahl Z von der Anwenderchipkarte AKi über die Kartenleseeinheit KL2 gelesen, und mittels der in den Speicher S der Lizenzchipkarte LK geladen.

Vom Prozessor P der Lizenzchipkarte LK wird dann für den Fall, daß die Anzahl der im nichtflüchtigen Speicher S enthaltenen, freischaltbaren Anwenderchipkarten AKn noch nicht erschöpft ist, eine von der jeweiligen Zufallszahl abhängige Freigabekennung FDi(Z) generiert, über die Kartenleseeinheit KL1 in die Schreib-Lesestation AKG geladen und schließlich über die Kartenleseeinheit KL2 in die Anwenderchipkarte AKi rückgeschrieben. Vom Prozessor P der Anwenderchipkarte AKi wird die Freigabekennung FDi auf Korrespondenz mit der Zufallszahl überprüft und bei positivem Ausgang der Prüfung eine Aktivierung des gesamten Satz zulässiger Anwenderbefehlsanweisungen bewirkt. Für den Fall, daß die Anzahl freigebbarer Anwenderchipkarten verbraucht ist, wird von der Lizenzchipkarte entweder kein Freigabekennung oder eine ungültige, d. h. in z. B. einer unzulässigen Weise mit der Zufallszahl verknüpfte Freigabekennung an die anfordernde Anwenderchipkarte übermittelt.

Bei dieser Ausführung der Erfindung aktivieren sich somit die Anwenderchipkarten AKn nach erfolgreichem Empfang einer zulässigen Freigabekennung selbst.

Die Erfindung weist somit den doppelten Vorteil auf, daß Anwenderchipkarten einerseits vor einer Freischaltung vollkommen unbrauchbar sind, und andererseits die Freischaltung von Anwenderchipkarten mit Hilfe des Systems der Lizenzchipkarte in einem eng begrenzbaren Rahmen genau überwachbar ist.

Bei einer anderen Ausführung des erfindungsgemäßen Chipkartensystems erfolgt die Freischaltung einer Anwenderchipkarte AKi durch Übertragung eines vom Betriebssystem für die Ausführung von Anwenderbefehlsanweisungen benötigten Freigabedatensatzes in den nichtflüchtigen Speicher der Anwenderchipkarte AKi über die Schreib-Lesestation AKG. In diesem Fall sind die Anwenderchipkarten nicht in der Lage, sich selbst zu aktivieren. Vielmehr wird der Freigabedatensatz für die Erreichung der vollen Funktionsfähigkeit zwingend benötigt.

In diesem Fall wird vom Prozessor P einer Anwenderchipkarte AKi zur Auslösung einer Freischaltung vorteilhaft wiederum zunächst eine Anforderung auf Übermittlung eines Freigabedatensatzes FDi mittels der Schreib-Lesestation AK an die Lizenzchipkarte (LK) übertragen. Vom Prozessor P der Lizenzchipkarte LK wird dann für den Fall, daß die Anzahl freischaltbarer Anwenderchipkarten AKn im nichtflüchtigen Speicher S noch nicht erschöpft ist, ein Freigabedatensatz FDi abgerufen bzw. generiert und wiederum mittels der Schreib-Lesestation AKG an die Anwenderchipkarte AKi übertragen. Dieser wird vom Prozessor P der Anwenderchipkarte AKi schließlich zur Ermöglichung des Betriebs des gesamten Satzes zulässiger Anwenderbefehlsanweisungen des Betriebssystems in den zumindest das Betriebssystem der Anwenderchipkarte AKi enthaltenden nichtflüchtigen Speicher S ordnungsgemäß eingebunden.

Bei dieser Ausführung der Erfindung ist die Sicherheit gegenüber unzulässigen Manipulationen weiter verbessert, da die Anwenderchipkarten ohne einen gegebenenfalls zusätzlich auf die jeweilige Anwenderchipkarte individualisierte Freigabedatensatz datentechnisch kei-

nesfalls funktionsfähig sind und somit auch nicht in einer unbefugten Weise freigeschaltet werden können.

Diese Ausführung des erfindungsgemäßen Chipkartensystems wird nachfolgend unter Heranziehung des Beispieles von Fig. 2 näher erläutert. Dabei dient als Freigabedatensatz bevorzugt eine betriebssystemspezifische Kommandotabelle KTB im nichtflüchtigen Programmspeicher S des Prozessors dient, womit die Zuordnung adr 1 ... adr k ... adr n von Anwenderbefehlsanweisungen AWB x zu den diese jeweils ausführenden Teilen des Betriebssystems BSC der Anwenderchipkarte AKi hergestellt wird.

Darüber hinausgehend kann es vorteilhaft sein, wenn der interne Prozessor P und ein zur Aufnahme eines Betriebssystems zum Betrieb des Prozessors P, und hierüber wiederum gegebenenfalls weiterer Funktionselemente der Anwenderchipkarte, wie z. B. Energieversorgung, Datenschnittstelle zum Austausch von Daten zwischen der Chipkarte und externen Schreib- und Lesestationen u. dgl., dienender nichtflüchtiger Programmspeicher S so aufeinander abgestimmt, daß die Anwenderchipkarte nach ihrer Herstellung nur eine Befehlsanweisung ausführen kann, wenn sie erstmalig mit einer Schreib-Lesestation in datentechnische Verbindung gebracht wird. Diese Befehlsanweisung bewirkt das Nachladen einer betriebssystemspezifischen Kommandotabelle in den nichtflüchtigen Speicher des Prozessors. Erst nach erfolgreicher Beendigung dieser La-deoperation ist eine Zuordnung von weiteren, insbesondere über externe Schreib-Lesestationen der Anwenderchipkarte zugeführten Anwenderbefehlsanweisungen zu den für deren Ausführung vorgesehenen, jeweiligen Betriebssystemteilen möglich. Die Ausführung der für eine ordnungsgemäße Funktionsfähigkeit der Anwenderchipkarte gehörigen Befehlsanweisungen in Bezug auf alle während der Normalnutzung maximal möglichen Operationen ist somit erst nach Einbindung der Kommandotabelle möglich.

Diese Ausführung bietet den Vorteil, daß u. U. auch sehr große Mengen frisch hergestellter Anwenderchipkarten nahezu vollkommen unbrauchbar sind. Die Ermöglichung der Gebrauchsfertigkeit erfolgt vielmehr separat für jede einzelne Chipkarte meist erst unmittelbar vor deren Übergabe an den berechtigten Endbenutzer. Neu hergestellte Chipkarten, in deren nichtflüchtigem Speicher bzw. anderen Speicherbereichen zwar die Codierung der aufeinanderfolgenden Betriebssystembefehlsanweisungen geladen ist, sind deswegen nicht funktionsfähig, weil aufgrund der fehlenden Kommandotabelle eingehende Anwenderbefehlsanweisungen nicht identifiziert und der bzw. die zu deren Ausführung benötigten Betriebssystemteile wegen der nicht vorhandenen, dazugehörigen Verzweigadressen nicht aktiviert werden können. Praktisch ist es mit vernünftigem Zeit- und Mittelaufwand nahezu nicht möglich, in der Art eines Reverse-Engineering die funktionelle Struktur des Betriebssystems so zu rekonstruieren, daß die zur Ausführung einzelner Anwenderbefehlsanweisung gehörigen Teile und deren mögliche Wechselwirkungen in Form von Einsprungadressen zugänglich werden.

Die Gestaltung einer Anwenderchipkarte gemäß dieser Ausführung der Erfindung bietet den Vorteil, daß die Chipkarte vor deren Autorisierung durch Nachladen der Kommandotabelle meist unmittelbar vor Übergabe in den Herrschaftsbereich des neuen Besitzers nahezu gegen jede Art von unbefugtem Gebrauch geschützt ist, ohne daß aufwendige Maßnahmen im Hard- oder Softwarebereich der Chipkarte vorgesehen werden müßten.

welche die Herstellung der Chipkarte verteuern und deren Gebrauchsfähigkeit möglicherweise einschränken würden. Einerseits ist auf einfache Weise möglich, die Chipkarte zur alleinigen Ausführbarkeit des Ladebefehls für die Kommandotabelle zu ertüchtigen. Andererseits bereitet das Nachladen der Kommandotabelle datentechnisch für eine befugterweise im Besitz des Codes der Kommandotabelle befindliche Einrichtung, wie z. B. eine Bank, keinerlei Probleme. Bei diesem Vorgang können bei Bedarf gleichzeitig auch beliebige weitere, die jeweilige Chipkarte z. B. bezüglich des neuen Benutzers individualisierende Daten übertragen werden.

Neben der Verhinderung unbefugter Benutzung von Anwenderchipkarten vor deren Übergabe in den normalen Gebrauch wird durch die Erfindung auch unterbunden, daß in dieser Zwischenphase in den bei der Herstellung auf die Anwenderchipkarten aufgebrachten Programmcode selbst, insbesondere der Code des Betriebssystems, in unbefugter Weise Einsicht genommen bzw. dieser unbefugt oder unprofessionell verändert wird.

Zur Erläuterung ist auf der rechten Seite der Fig. 2 beispielhaft in anschaulicher Tabellenform ein Ausschnitt aus der Sequenz der aufeinanderfolgenden Anweisungen eines Betriebssystemcodes BSC dargestellt. 25 Dabei ist gedanklich die Tabelle sowohl nach oben als auch nach unten fortzusetzen. Der Ausschnitt zeigt beispielhaft eine vorangehende Einsprungadresse adr k-1 und eine darauf folgende Einsprungadresse adr k. Die einer dieser Einsprungadressen zugeordnete Zeile des 30 Betriebssystembefehlscodes und die bis zur nächsten Einsprungadresse darauf folgenden Zeilen des Betriebssystembefehlscodes bilden eine Gruppe, welche die Ausführung eines bestimmten Anwenderkommandos bewirkt.

Im Beispiel der Fig. 2 wird der Anwenderchipkarte ein aktuelles Anwenderkommando AWB x bevorzugt von einer externen Schreib-Lesestation zugeführt. Dieses soll vom Betriebssystem ausgeführt werden. Hierzu wird eine Kommandotabelle KTB benötigt, welche quasi einen den Zugang zu den funktionellen Teileinheiten des Betriebssystems BSC ermöglichenen Schlüssel darstellt. Beispieldarstellung besteht jede Zeile der Kommandotabelle KTB aus einem ersten Codeteil bic k, welcher zur Interpretation, d. h. zur Erkennung des Typs, des 40 aktuellen Anwenderkommandos AWB x dient, und aus einem zweiten Codeteil adr k, welcher die Startadresse der dazugehörigen Betriebssystembefehlssequenz enthält. Die Kommandotabelle KTB besteht somit aus einer ersten Teiltabelle BIT, welche die zur Befehlsinterpretation dienenden Codes bic 1, bic 2, bic 3 ... bic k ... 45 bic n-1, bic n enthält, und aus einer zweiten Teiltabelle BSC, welche die dazugehörigen Einsprungadressen adr 1, adr 2, adr 3 ... adr k ... adr n-1, adr n der entsprechenden Betriebssystemsequenzen enthält.

Bei dem in der Fig. 2 dargestellten Beispiel wird ein mit AWB x bezeichnetes Anwenderkommando der Anwenderchipkarte zugeführt. Dieses wird durch die Codierung bic k als zulässiger Befehl erkannt, was in der Figur durch eine strichlierte Linie auf der linken Seite der Kommandotabelle KTB dargestellt ist. Nun wird die dazugehörige Einsprungadresse adr k aktiviert und hierdurch der Code des Betriebssystems BSC von Beginn bei der Einsprungadresse adr k an ausgeführt. In der Figur ist der Aufruf der zum Anwenderkommando AWB x gehörenden Betriebssystemsequenz durch einen von der entsprechenden Zelle der Kommandotabelle KTB bis zur Einsprungadresse adr k verlaufenden Pfeil 55

SBS dargestellt. Es ist zu erkennen, daß ohne die Brückenfunktion einer Kommandotabelle KTB kein Anwenderkommando AWB x ausführbar ist, da keine Zuordnung desselben zu dem dazugehörigen Teil des Betriebssystems möglich ist. Diese erfindungsgemäße Ausgestaltung einer Anwenderchipkarte stellt somit einen außerordentlich wirksamen Schutz gegen unbefugte Benutzung frisch hergestellter Chipkarten dar.

Schließlich kann der Datenaustausch zwischen einer 10 Anwenderchipkarte AKi und der Lizenzchipkarte (LK) mittels der Schreib-Lesestation AKG vorteilhaft in einer kryptologisch verschlüsselten Form erfolgen.

Patentansprüche

1. Chipkartensystem, dessen Chipkarten (AK, LK) jeweils mindestens einen internen Prozessor (P) und einen nichtflüchtigen Speicher (S) zumindest für ein Betriebssystem des Prozessors (P) aufweisen, mit

1.1 einer Vielzahl von Anwenderchipkarten (AKn), deren Prozessor (P) jeweils erst nach einer Freischaltung Anwenderbefehlsanweisungen ausführen kann,

1.2 zumindest einer Lizenzchipkarte (LK), in deren nichtflüchtigen Speicher (S) eine begrenzbare Anzahl von freischaltbaren Anwenderchipkarten (AKn) verwaltbar ist, und mit

1.3 mindestens einer Schreib-Lesestation (AKG) für Chipkarten (LK), worüber

1.3.1 in einer Anwenderchipkarte (AKi) die Freischaltung des internen Prozessors (P) wirkt wird, wenn im Speicher (S) der Lizenzchipkarte (LK) die Anzahl der freischaltbaren Anwenderchipkarten (AKn) noch nicht erschöpft ist, und

1.3.2 im Speicher (S) der Lizenzchipkarte (LK) eine Dekrementierung der Anzahl freischaltbarer Anwenderchipkarten (AKn) bewirkt wird.

2. Chipkartensystem nach Anspruch 1, wobei die mindestens eine Lizenzchipkarte (LK) und die Anwenderchipkarten (AKn) hardwaremäßig identisch sind.

3. Chipkartensystem nach Anspruch 1 oder 2, wobei

3.1 vom Prozessor (P) einer Anwenderchipkarte (AKi) zur Auslösung einer Freischaltung zunächst eine Zufallszahl erzeugt und mittels der Schreib-Lesestation (AKG) an die Lizenzchipkarte (LK) übertragen wird,

3.2 vom Prozessor (P) der Lizenzchipkarte (LK) für den Fall, daß die Anzahl freischaltbarer Anwenderchipkarten (AKn) im Speicher (S) noch nicht erschöpft ist, eine von der jeweiligen Zufallszahl abhängige Freigabekennung (FDi) generiert und mittels der Schreib-Lesestation (AKG) an die Anwenderchipkarte (AKi) übertragen wird, und

3.3 vom Prozessor (P) der Anwenderchipkarte (AKi) die Freigabekennung (FDi) auf Korrespondenz mit der Zufallszahl überprüft und bei positivem Ausgang der Prüfung eine Aktivierung des gesamten Satz zulässiger Anwenderbefehlsanweisungen bewirkt wird.

4. Chipkartensystem nach einem der Ansprüche 1 oder 2, wobei die Freischaltung einer Anwenderchipkarte (AKi) durch Übertragung eines vom Betriebssystem für die Ausführung von Anwenderbe-

fehlsanweisungen benötigten Freigabedatensatzes
in den nichtflüchtigen Speicher der Anwenderchip-
karte (AKi) über die Schreib-Lesestation (AKG)
erfolgt.

5. Chipkartensystem nach Anspruch 3, wobei

5.1 vom Prozessor (P) einer Anwenderchipkar-
te (AKi) zur Auslösung einer Freischaltung zu-
nächst eine Anforderung auf Übermittlung ei-
nes Freigabedatensatzes (FDi) mittels der
Schreib-Lesestation (AKG) an die Lizenzchip-
karte (LK) übertragen wird,

5.2 vom Prozessor (P) der Lizenzchipkarte
(LK) für den Fall, daß die Anzahl freischaltba-
rer Anwenderchipkarten (AKn) im Speicher
(S) noch nicht erschöpft ist, ein Freigabedaten-
satz (FDi) generiert und mittels der Schreib-
Lesestation (AKG) an die Anwenderchipkarte
(AKi) übertragen wird, und

5.3 vom Prozessor (P) der Anwenderchipkarte
(AKi) der Freigabedatensatz zur Aktivierung 20
des gesamten Satzes an zulässigen Anwender-
befehlsanweisungen des Betriebssystems in
den zumindest das Betriebssystem der Anwen-
derchipkarte (AKi) enthaltenden nichtflüchtig-
en Speicher (S) für geladen wird.

6. Chipkartensystem nach Anspruch 4 oder 5, wobei
als Freigabedatensatz eine betriebssystemspezifi-
sche Kommandotabelle (KTB) im nichtflüchtigen
Programmspeicher des Prozessors dient, womit die
Zuordnung (adr 1 ... adr k ... adr n) von Anwender-
befehlsanweisungen (AWB x) zu den diese jeweils
ausführenden Teilen des Betriebssystems (BSC) der
Anwenderchipkarte (AKi) hergestellt wird.

7. Chipkartensystem nach einem der vorangegan-
genen Ansprüche, wobei der Datenaustausch zwi-
schen einer Anwenderchipkarte (AKi) und der Li-
enzchipkarte (LK) mittels der Schreib-Lesestation
(AKG) in einer kryptologisch verschlüsselten Form
erfolgt.

Hierzu 2 Seite(n) Zeichnungen

40

45

50

55

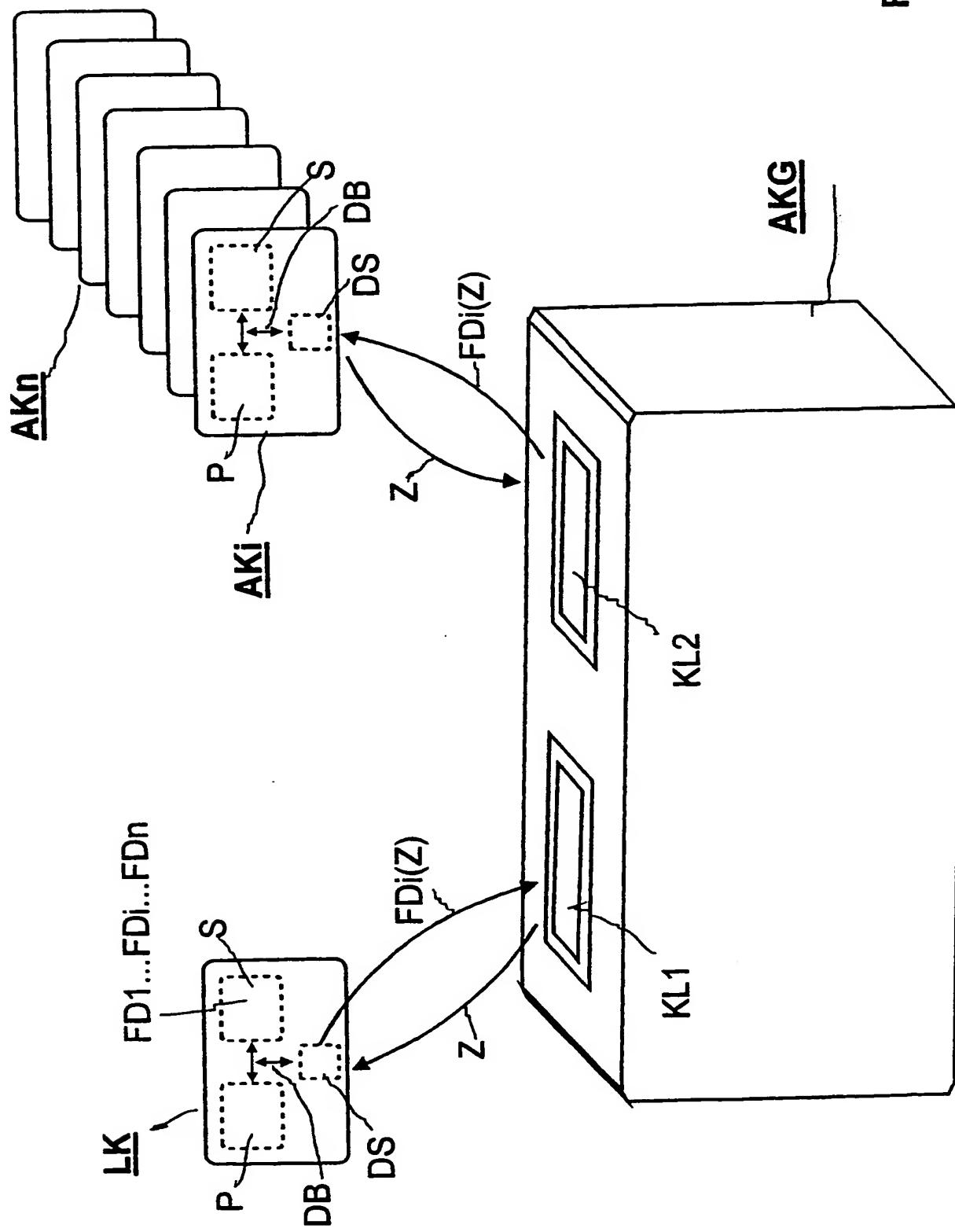
60

65

BEST AVAILABLE COPY

- Leerseite -

FIG 1



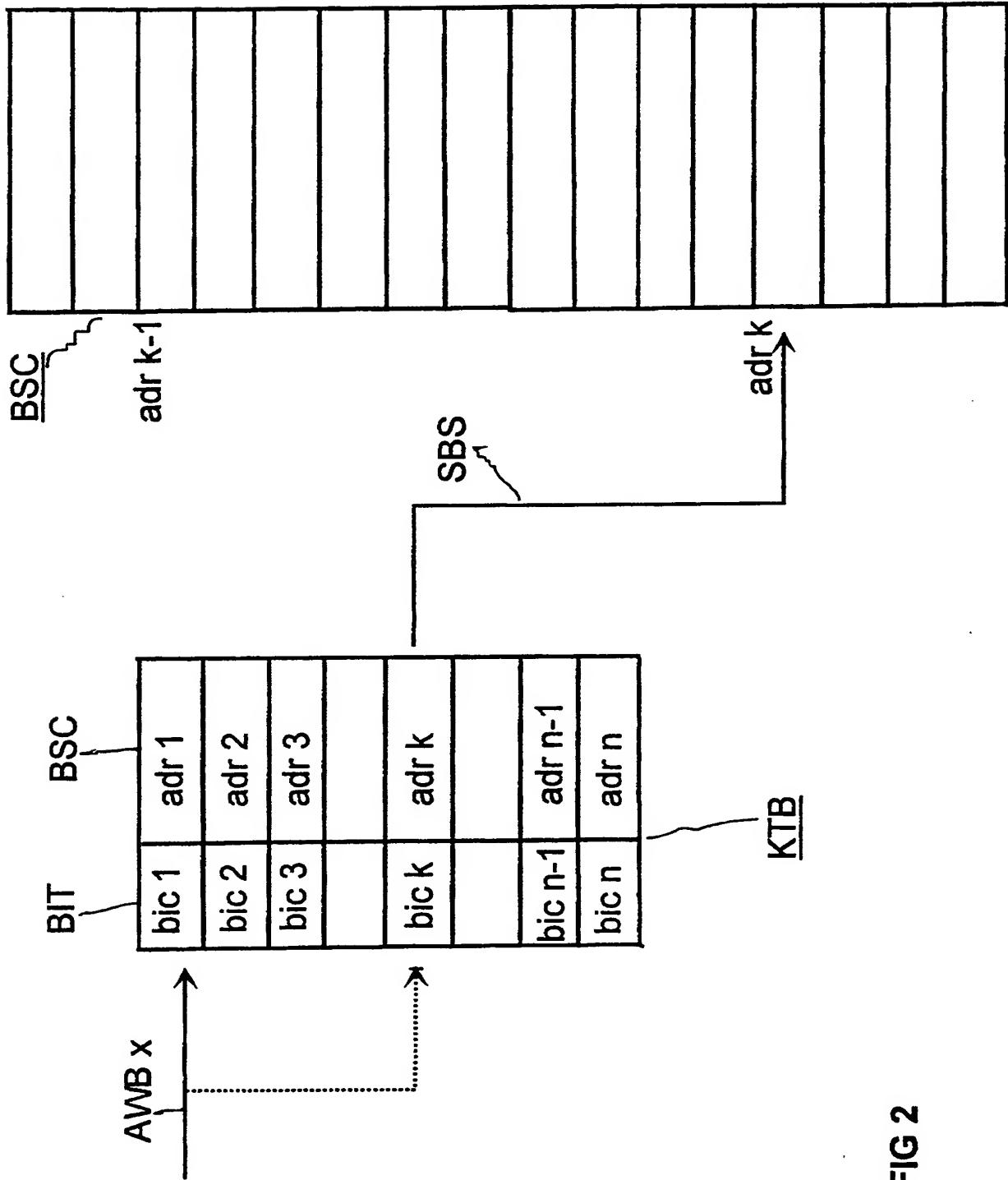


FIG 2